ManageEngine
Log360

Using MITRE ATT&CK®

to understand the techniques behind **2023's biggest breaches**

What we can learn from past breaches
to step up our security defense mechanisms

Introduction

In the age of digital interconnectedness, the value and vulnerability of data has never been more apparent. Data breaches have become an all too familiar threat, posing significant risks to individuals, organizations, and the integrity of sensitive information.

Among the numerous data breaches that have shaken the digital landscape, the 2023 data breach of Reddit stood out as one of the most prominent and concerning incidents at the start of the year. Reddit, the popular social media platform with millions of users, fell victim to a sophisticated cyberattack that targeted its vast treasure trove of user information. The breach exposed "limited contact information for (currently hundreds of) company contacts and employees (current and former), as well as limited advertiser information," said Reddit in its statement.

About the breach

The breach was claimed by BlackCat ransomware gang (also known as ALPHV), who claim to have stolen 80GB of sensitive data and threatened to release the stolen information.

In addition to Reddit, another company that recently fell victim to BlackCat ransomware is healthcare giant Henry Schein. On October 15, 2023, Henry Schein disclosed that it had experienced a cybersecurity incident. The BlackCat group subsequently claimed responsibility for the attack, revealing that it had successfully breached the company's network and exfiltrated approximately 35TB of sensitive files. The BlackCat ransomware also targeted McLaren Health Care and Seiko, putting personal data at risk of exposure.

The aftermath of these data breaches serves as a stark reminder of the far-reaching implications of such security lapses. The breaches sparked concerns of identity theft, phishing attacks and potential compromise of other online accounts for affected users.

The data breaches also exemplify the urgency for individuals and organizations to prioritize data protection and adopt robust cybersecurity measures. As technology continues to advance, so do the tactics of cybercriminals. In this whitepaper, we will attempt to decode the attack techniques behind the BlackCat data breaches, and the best way to understand attack patterns is by mapping them to the MITRE ATT&CK Matrix.

What is the MITRE ATT&CK framework?

What is the MITRE ATT&CK framework?

The MITRE ATT&CK framework is a comprehensive model of tactics and techniques used by attackers that helps security teams identify patterns in the attack methodology for quick threat detection and investigation. There may be many cyberthreats lurking at any given moment, but the techniques used by attackers are not as varied.

The MITRE ATT&CK threat modelling framework helps security teams develop a robust cybersecurity infrastructure, as it not only identifies the techniques and possible steps the attacker could take, but explains the ways in which these techniques can be detected and mitigated. Here are some ways that it can help your business:

Threat detection and prevention: Businesses can better understand how attackers operate by mapping real-world attacks to the MITRE ATT&CK framework. This knowledge is invaluable for detecting and preventing similar attacks in the future.

Incident response and forensics: In the case of an incident or data breach, it provides a framework for security teams to assess the situation quickly, identify the tactics and techniques used, and the type of data that may have been compromised. This allows for effective incident response.

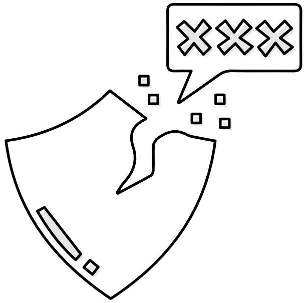
Gap analysis and security posture improvement: Businesses can compare their security measures against the MITRE ATT&CK framework to identify the gaps in their defenses and identify the areas they need to prioritize.

Vendor evaluation and security tooling: Businesses can also use the framework when selecting cybersecurity tools and solutions. It allows you to asses how well the solution can tackle various attack techniques and make an informed decision on whether the vendor will help your business requirements.

Regulatory and compliance requirements: Many regulatory bodies and compliance standards require organizations to have robust cybersecurity measures in place. Mapping security controls and practices to the MITRE ATT&CK framework can help demonstrate compliance with these requirements.

This whitepaper maps the BlackCat ransomware attack pattern to MITRE ATT&CK's tactics, techniques, and procedures (TTP) to understand its attack pattern along with what you can do to mitigate such an attack.

Mapping the BlackCat ransomware attack pattern with **MITRE ATT&CK** threat modelling framework techniques



The BlackCat ransomware gang's attack usually starts with a sophisticated phishing attack. The malware is coded in the Rust programming language, which helps them evade malware detection systems. This is because solutions look for languages that are well-known and widely used. Rust, being a new language, helps the BlackCat ransomware evade detection mechanisms. This allows them to elevate privileges and gain unauthorized access to files, which the ransomware group then encrypts and threatens to leak.

Technique

Phishing (T1566): Phishing is a commonly used technique that attackers use to gain initial access into a network. Cybercriminals use unassuming emails that contain malicious attachments or links that, once clicked or downloaded, execute the malicious code on the victim's systems.

How threat actors leverage this technique

This is the technique used by the BlackCat group to gain their initial foothold in the network. In their statement, Reddit claimed that it was a "sophisticated and highly-targeted phishing attack", where the threat actor sent out "plausible sounding prompts" to their employees, which led them to a website that cloned the behavior of Reddit's intranet gateway.

Technique

Access Token Manipulation (T1134): In this technique, threat actors modify access tokens and operate under a different user to gain authorized access to information. By manipulating the access token, they can make a running process appear as if it is the child of a different process, or belongs to a different user. The process then takes on the security context of the new user. This technique is difficult to detect as the user access will look legitimate.

How threat actors leverage this technique

The BlackCat ransomware is a malicious software that comes in the form of a command-line tool. The ransomware requires an access token (a 32-character code) to run. Without this token, the ransomware won't execute, making it difficult for security researchers or automated analysis tools to study it in a safe environment.

The ransomware uses the **GetCommandLineW** API to check if the access token is provided correctly. Once provided with the 32-character code, the ransomware starts its malicious activities.

Technique

Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002): Attackers attempt to elevate their privileges on a system by bypassing User Access Control (UAC) mechanisms. Windows UAC allows a user to perform a task with administrator privileges by prompting the user for confirmation with a consent prompt. If the UAC protection isn't set to the highest level, attackers can exploit Component Object Model (COM) objects to avoid triggering the UAC prompt and gain access to administrative privileges.

How threat actors leverage this technique

The BlackCat ransomware exploits COM objects used by the Microsoft Connection Manager Profile Installer (CMSTP) binary, particularly the **CMSTPLUA** interface **{3E5FC7F9-9A51-4367-9063-A120244FBEC7}**. This is an example of dynamic link library (DLL) hijacking.

It uses **CoGetObject** to register the malicious DLL with the **CLSID {3E5FC7F9-9A51-4367-9063-A120244FBEC7}**, and this malicious DLL loads and runs when called for by the CMSTP with elevated privileges. This technique allows the BlackCat ransomware to bypass the UAC prompt and perform its malicious actions without being detected or blocked by the system's security measures.

Technique

Permission Groups Discovery: Domain Groups (T1069.002): Attackers can attempt to discover the domain-level groups and permission settings to give themselves elevated privileges.

How threat actors leverage this technique

Once the BlackCat ransomware bypasses the UAC, it uses the **LookupPrivilegeValueW** API to look for the list of privileges. These privileges would allow the process to run system-level operations. **AdjustTokenPrivileges** is then used to grant the attacker those privileges.

Now, the ransomware gets ready to encrypt the victim's files and make them inaccessible. However, before doing so, it takes some precautionary steps to hinder any recovery attempts.

Technique

Inhibit System Recovery (T1490): In this technique, attackers can disable services that are designed to help in the backup and recovery of corrupted systems. This can be executed with native Windows utilities.

How threat actors leverage this technique

To ensure that the victim would not be able to recover the files, the malicious software executes the following steps:

a. It deletes volume shadow copies using **vssadmin** and **wmic** commads, which are backups of files that could be used to restore data.

b. It disables Automatic Repair using **bcdedit**, preventing the system from repairing itself after an attack.

c. It clears event logs, which could contain valuable information about the ransomware's actions.

d. It terminates active services and processes, potentially to avoid detection or interference.

Technique

File and Directory Discovery (T1083): Threat actors may list out files and directories, or look for particular information within a file system and encrypt those files. This can be carried out by many commands.

How threat actors leverage this technique

The BlackCat ransomware uses **FindFirstFile** and **FindNextFile** to find all the files on the system. **WriteFile** is then used to write the ransom note in each directory.

Technique

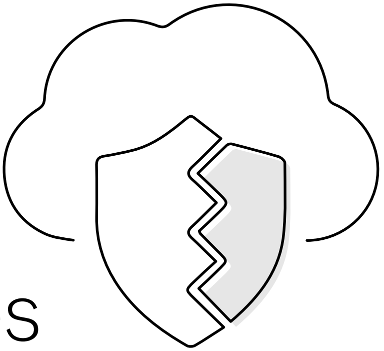
Data Encrypted for Impact (T1486): After gaining access to the targeted files, attackers render the files inaccessible by encrypting them, and withholding the decryption key.

How threat actors leverage this technique

The BlackCat ransomware generates a secret key using a special algorithm called Advanced Encryption Standard (AES). This secret key is like a password that only the ransomware knows.It's used to lock up your files securely and is given to the ransomware victim to decrypt their files.

Once the targeted files in the system are encrypted, the victim's desktop wallpaper is changed, asking them to refer to the ransom note to regain access to their files.

Lessons from the **biggest data breaches of 2023** and how they can be used to step up our defenses



A multi-layered security approach is required to detect and defend against a cyberattack similar to the BlackCat ransomware. Below are some detection techniques and best practices that can help mitigate the risk of such an attack:

1

Anomaly detection and behavior monitoring:

- Implement behavior-based anomaly detection systems that can identify unusual process behaviors, such as a process attempting to encrypt multiple files rapidly.
- Use security tools such as SIEM solutions to detect unauthorized or suspicious process creations and privilege escalation attempts. Techniques such as UAC bypass can be difficult to detect with normal rule-based detection systems. A behavior-based approach, such as user and entity behavior analytics (UEBA), sets a baseline for normal behavior which helps detect any anomalous behavior instantly.

2

Network traffic analysis:

- Monitor network traffic for unusual or large volumes of data being transferred to external destinations, as ransomware may exfiltrate data during its execution. This can be done with the help of behavioral analytics, to set a baseline of normal network traffic and detect abnormal network traffic. These solutions would gather an understanding of regular data transfers (including volume and type of data being transferred) and would alert you of any anomalies for quick detection and response.

3

File system monitoring

- Employ file system monitoring tools to watch for numerous files being modified (encrypted) within a short period.
- Implement file integrity monitoring (FIM) to detect unauthorized modifications to critical files.

4

Privilege escalation monitoring:

- Monitor for suspicious calls to API functions like **LookupPrivilegeValueW** and **AdjustTokenPrivileges**, as these may indicate privilege escalation attempts.

5

Threat intelligence and behavioral analysis:

- Stay informed about the latest ransomware threats and their techniques through threat intelligence sources.
- Use behavioral analysis to identify unusual patterns and characteristics associated with known ransomware families, like BlackCat.

6

Email and web security:

- Implement strong email security gateways that can block phishing attempts and malicious attachments containing ransomware.
- Use web filtering to prevent access to known malicious websites used in ransomware distribution.

7

Least privilege and segmentation:

- Apply the principle of least privilege to limit the permissions of users and processes on the system.
- Segment your network to prevent lateral movement of ransomware within the network.

How to prevent attacks similar to **BlackCat ransomware attack**

Mitigating an attack by the BlackCat ransomware group or similar ransomware threats involves implementing a combination of technical measures and best practices to enhance your organization's security posture. Here are some key steps to mitigate the risk of such an attack:

- **User awareness training:** Educate your employees on ransomware threats, phishing techniques, and safe computing practices to make them more aware of the cyberthreats that are prevalent. Encourage them to be cautious with email links and attachments, to avoid the risk of phishing, or other social engineering attacks.
- **Zero Trust implementation:** Enforce the principle of least privilege, ensuring that users and processes only have the minimum necessary permissions to perform their tasks. It is recommended to follow the Zero Trust security model, which promotes continuous verification, least privilege, end-to-end encryption, and the use of analytics to minimize the impact of a breach.
- **User account management:** Manage the creation, modification, and permissions of user accounts based on need to reduce the risk of lateral movement and to keep your resources secure.
- **Network segmentation:** Segment your network to separate critical assets and resources, to limit the impact of lateral movement in the event of a breach.
- **Multi-factor authentication (MFA):** Enable MFA wherever possible to add an extra layer of security to user accounts.
- **Regular security assessments and audits:** Conduct regular security assessments of systems, insecure software and configurations, and permissions, and conduct penetration testing to identify and address any vulnerabilities.
- **Monitor for anomalies:** Monitor network and endpoint activities for unusual behavior or signs of compromise. Use intrusion detection systems to block any threats to the network before they gain initial foothold.
- **Data backup:** Take and store regular backups from critical servers and ensure that they're secure. It is recommended to harden the security of this backup, and store it separately from the corporate network to limit the chances of compromise.
- **Data loss prevention (DLP):** Implement a data loss prevention strategy to categorize your data, identify sensitive information, and prevent the exfiltration of data.
- **Security information and event management (SIEM):** Implement a SIEM solution to centralize and analyze security event logs for early detection of suspicious activities.

Conclusion

The BlackCat data breaches highlighted the importance of having a robust security posture and incident management system in place, as an attack can happen at any given time. Any malicious link or accidental download can have severe consequences and heavily cost the organization–either financially or in terms of their reputation.

The breaches emphasized the need for companies to invest in their security infrastructure, conduct regular security assessments, and stay vigilant against emerging threats. However, continuously monitoring for threats and suspicious events can be hard to do, which is what attackers rely on. This difficulty can be overcome by investing in a security tool that monitors, detects, and flags potential threats instantly to prevent the attack from escalating.

About ManageEngine's SIEM:

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates, and responds to security threats. It combines threat intelligence, machine learning-based anomaly detection, and rule-based attack detection techniques to detect sophisticated attacks, and offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud, and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

$ Get Quote

⭳ Download

Here's how **Log360 can help** you with:

- Attack detection
- Intrusion detection
- Detect malware
- Detect APTs using MITRE ATT&CK framework
- Spotting privilege escalation
- Detect changes to sensitive data